International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Versatile Digital Identity

Shaik Abdulla [1]

[1]*B. Tech Student, Department of Information Technology, GMR Institute of Technology, Vizianagaram District, A.P, India*

ABSTRACT

Blockchain is an ever-growing distributed cryptographically secured immutable ledger which is the foundation of a decentralized future. First established in 2008 by Satoshi Nakamoto in the Bitcoin whitepaper, Blockchain has evolved in many ways allowing for the storage and operation of computer code which then ensures complete trust in the applications built on this technology. The number of individuals with a digital presence has greatly increased over the last ten years, and there are now billions of linked devices, people, and items, making communication more simpler than it ever was. The provision of Digital Identities has become essential for establishing this link in the digital age. This project presents an innovative proposal for everyone to own their own Digital Identity which works as a replacement for Aadhar card, PAN card, Driving License, Passport, Voter ID and any other typical identity or authorization documents. This is created by ERC-721 token standard of Ethereum blockchain to mint an NFT which is publicly verifiable and the necessary files are stored on IPFS. The user can authorize the verification of the necessities and hide the unrequired details. This verification process can be done using a Smart Contract which ensures security and validity. This makes the identities visible to no one but verifiable by everyone.

Keywords: Blockchain, Distributed, Immutable, Decentralized, Digital Identity, Ethereum, Smart Contract, Non-Fungible Token, InterPlanetary File System

INTRODUCTION:

In many organizations, the higher authority has the last say in all decisions. This indicates that the decision-making capacity decreases exponentially as we proceed down the pyramid. A centralized organization fits this description. On the other hand, in other organizations, the members at the lowest levels of the hierarchy are given a sizable portion of the decision-making cake. This system is decentralized, to put it simply. Decentralization also stresses putting power close to the action points while moving power down in the chain of command. One crucial thing to keep in mind is that the decision-maker is given a good deal of autonomy and responsibility here. Our officially issued government identities are a great concern for our privacy as it contains a lot of private information. These identities while in control of government are at the end of the day managed by human intervention and that puts our identities at risk. These identities could be relocated to Blockchain to make them decentralized. The authority over them could be given to the respective owners to update the access modifiers. The verification system could be automated using smart contracts. We use Blockchain because applications built on top of it are Open sourced, Trustless, Permissionless and most of all Decentralized.

1. Blockchain:

A blockchain is a shared, permanent database that resides on a computer network's numerous nodes. They save data in a way that renders system modification or hacking probabilistically difficult. Specifically, blockchain records data as a chain of blocks, as suggested by its name. Each block consists of a collection of transactions, some of which may involve moving assets around the network and others which may involve changing the data kept on the blockchain.

When the Bitcoin Network was released in 2009, the unidentified individual (or group) known as Satoshi Nakamoto popularised blockchain technology. Bitcoin is a cryptocurrency network that primarily manages the transfer of the BTC assets across the network without the need of a reliable middleman or authority, all the while keeping the network safe and impenetrable to hacking. Blockchains have a Genesis State when they first start. When the public network first debuted in 2009, Bitcoin entered its genesis state. When Ethereum was debuted in 2015, this was its Genesis State. On a blockchain, each transaction updates the shared state that is copied by all nodes. Due to the massive volume of transactions, blocks of transactions are formed. Thus, the name. These blocks are chained together in a historical traceable pattern that can be cryptographically validated. A network's current state can be updated at any moment by beginning with the genesis block and transitioning the state in accordance with the data included in each subsequent block.

1.1 Node:

An autonomous peer-to-peer distributed network of computer nodes administers a blockchain network. You may conceive of each node in the network as keeping a copy of the global transaction ledger without delving into too much detail. As a result, each node may independently audit and validate all network transactions to make sure there was no fraudulent activity. Another kind of node, known as a mining node, is in charge of collecting fresh transactions made on a network into a block, validating them, and then submitting the block for inclusion onto the shared ledger by everyone else. Because mining is computationally challenging and crucial for maintaining security, those whose blocks are accepted receive a little reward for their efforts. The use of a blockchain proves that each unit of value was moved just once, and Satoshi Nakamoto's clever procedures eliminated the long-standing issue of decentralized multiple spending.

1.2 Decentralization:

The blockchain is a decentralized network because data is stored in a peer-to-peer network of nodes. Compared to the conventional method of centrally storing data, this has a number of advantages. There are several notable instances of centralization issues, some of which we are mentioned here:

- Centralized systems that experience data breaches disclose a lot of data
- Centralized authorities have the power to censor and suppress speech
- Reliance on a central authority results in downstream consumers being impacted by upstream issues.

Decentralization, on the other hand, has the opposite effect.

- No censorship because you cannot be censored by a single authority or middleman
- No downtime because the network is operating on thousands of nodes
- Highly attack-resistant, making data manipulation or destruction impossible

2. Ethereum:

Decentralized blockchain Ethereum is compatible with smart contracts. Ethereum is more multipurpose than Bitcoin, which simply supports the movement of the Bitcoin token inside the network.

On Ethereum, dApps are created using the Solidity programming language. Solidity allows you to create smart contracts and deploy them to the Ethereum Network. With Proof of Stake, it upholds consensus among all the computers in its network (PoS). Ethereum switched from a Proof of Work to a Proof of Stake mechanism in September of 2022 thanks to the Serenity Patch.

"Ether," often known as "ETH," is the native currency of Ethereum. To use the Ethereum network, you must use this token to pay the transaction fees.

2.1 Smart Contracts:

Without a central coordinator, all of the systems on the Ethereum network clone and execute smart contracts, which are simple computer programmes. You can design contracts employing smart contracts so that they can automatically be enforced by computer code. Any number of potential applications can be built on top of Ethereum thanks to its general-purpose design, and they will all inherit the security and decentralization advantages that come with using the Ethereum blockchain.

2.2 ERC20, ERC721 and ERC1155 Tokens:

On Ethereum, in addition to using Ether, users can develop and utilise their own currencies. ERC20 tokens are by far the most widely used type of currency. ERC20 Tokens are smart contracts that comply to a particular specification. Developers are free to go above the norm, but when creating their own tokens, they must abide to the basic standards. The standardization eliminates the need for unique coding for each new token by enabling digital wallets to support all token kinds with ease.

NFTs are another name for the ERC721 and ERC1155 standards. Similar to ERC20, these two standards set the minimum norms that must be met while developing NFTs. Additionally, because all NFT collections comply to one of these two standards, they automatically work with wallets and NFT marketplaces. They offer similar benefits.

2.3 Non-fungible tokens:

Cryptographic assets known as non-fungible tokens (NFTs) are distinguishable from one another on a blockchain by unique identification codes and relevant data. The crypto paradigm is changed by NFTs since it is impossible for two non-fungible tokens to be equal because each token is unique and un-replicable. They are digital representations of assets and have been likened to digital passports since each token has a unique, non-transferable identity that enables it to be identified from other tokens. Many companies, people, and artists desire to earn from their efforts, whether they are tweets or works of art. You may prove that you are the owner of a store of value by using digital artworks referred to as NFT artworks. An NFT marketplace is a virtual marketplace for buying and selling NFTs. Users may store, display, and sell their NFTs to other users on these sites in return for cryptocurrencies or cash. Customers can also directly mint NFTs on some NFT marketplaces' websites.

3. Web 3:

Using ideas like decentralization, blockchain technology, and token-based economics, Web3 proposes a new version of the World Wide Web. Some journalists and engineers have compared it to Web 2.0, where they claim that content and data are concentrated in a select few businesses that are frequently referred to as "Big Tech." Gavin Wood, a co-founder of Ethereum, popularized the phrase "Web3" in 2014, and venture capital firms, cryptocurrency enthusiasts, and major technological businesses began to show interest in the concept in 2021. Between web2 and web3, there are a few key distinctions, but decentralization is at their heart. With a few extra features, Web3 improves the internet as we now know it. web3 is Verifiable, Trustless, Self-governing, Permissionless, Distributed and robust, Stateful with Native built-in payments.

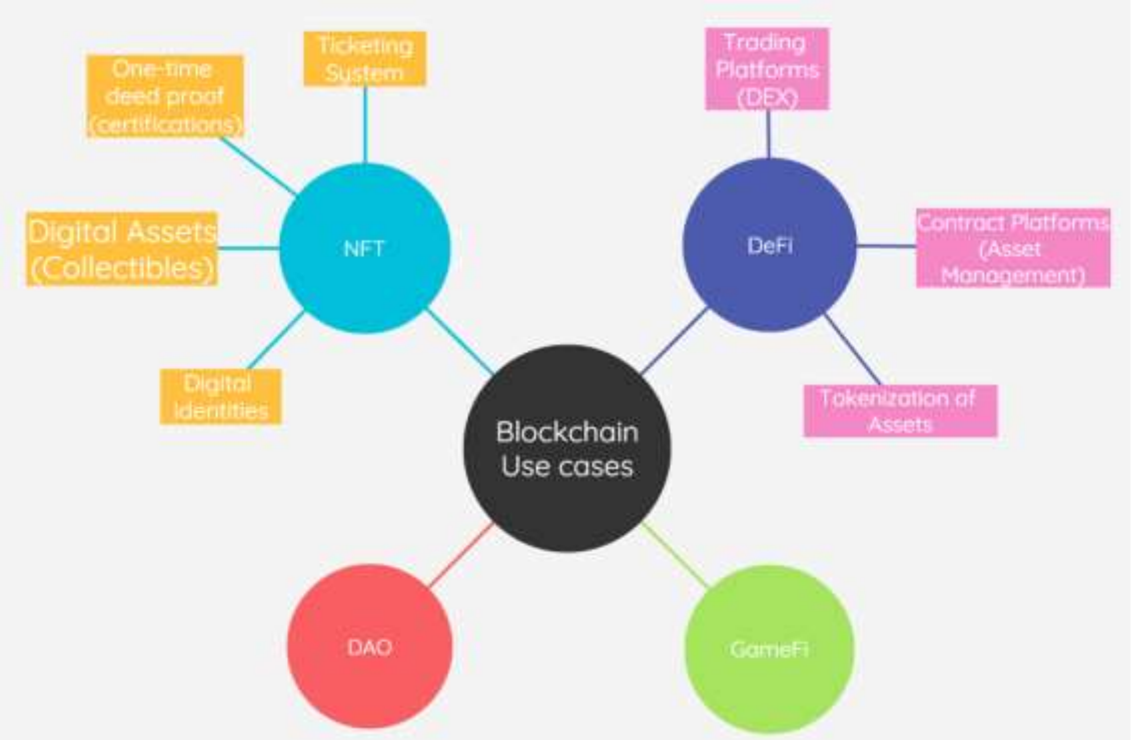

Fig. Overview of use cases of blockchain

3.1 IPFS:

In a distributed file system, data may be stored and shared using the InterPlanetary File System (IPFS), a protocol and peer-to-peer network. Each file in a global namespace connecting all computing devices is uniquely identified by IPFS via content-addressing (content identifier, or CID). Other nodes look up your file by asking their peer nodes where the content that the file's CID refers to is stored. They make a copy of your file when they view or download it, and until their cache is cleaned, they are another source of your content.

3.2 Digital Identity:

A digital identity is the collection of data online about a person, business, or piece of technology. It is feasible to identify persons or their devices using their unique identifiers and usage patterns.

A DI's entire lifecycle, including its creation, storage, authentication, authorization, revocation, and destruction, is defined by an identity management system (IMS). The three categories of identity solutions are centralized, federated, and decentralized. Since identity attributes in the centralized and federated systems are handled by a third party, such as an identity provider, they are referred to as classical systems. However, the decentralized system is the modern method of controlling digital identities, where users themselves control the qualities. A distinctive identifier that may be used in a decentral way must be created in order to create a decentralized identity. Decentralized Identifiers (DIDs) are identifiers that are established by the entities themselves, as opposed to conventional identifiers that are issued by the authority issuing the identification. Therefore, no centralized registry, identity provider, or certificate authority is dependent on DIDs.

LITERATURE SURVEY:

NFT's are unique and they could be anything in the digital world or we could take inspiration from the real world. In paper [2] P.Gellman in his "Blockchain: The New Art House" explained how he would make NFTs out of art work. Many companies, people and artists would show an interest in monetizing their creations from artworks. NFT artworks are digital art that allows one to prove the ownership of a store of value. A digital marketplace for purchasing and selling NFTs is known as an NFT marketplace. These platforms let users to store, show, and sell their NFTs to other users in exchange for cryptocurrencies or cash. On some NFT markets, consumers may mint their NFTs right there on the website. In paper [3] we see the use of IPFS in the streamflow data. It is essential to combine data into clusters and make it available to the public when acquiring streamflow from dispersed places and using a heterogeneous approach. When stored in distributed data processing nodes, time-series data must adhere to an in-out flowing water distribution system that requires traceability and comparison with the actual flow in order to be compliant. In Paper [3] we clearly see the topic of Identity Management. A DI's whole lifespan, including its creation, storage, authentication, authorization, revocation, and destruction, is defined by an IMS(Identity Management System). The three kinds of identity solutions are centralized, federated, and decentralized. Since identity attributes in the centralized and federated systems are handled by a third party, such as an identity provider, they are referred to as classical systems. However, the decentralized system is the modern method of controlling digital identities, where users themselves control the qualities. A distinctive identification that may be used in a decentralized way must be created in order to create a decentralized identity. Decentralized Identifiers (DIDs) are identifiers that are established by the entities themselves, as opposed to conventional identifiers that are issued by the authority granting the identification. Consequently, DIDs are not dependent on any centralized registry, identity provider, or a certificate authority. In paper [1] Weilin Zheng, Zheng, Xiangping Chen, Kemian Dai, Peishan Li and Renfei defined a BaaS(Blockchain as a Service) platform called NutBaaS. It provides BaaS over cloud computing environments, such as network deployment and system monitoring, smart contract analysis and testing. These services make it possible to create Dapps (Decentralized Apps), allowing developers to concentrate on the business code and investigate how to better use blockchain technology to their particular business situations without having to worry about maintaining and monitoring the system. In paper [5] Jagger S. Bellagrada and Adnan M. Abu-Mahfouz made a extensive survey on how the distributed ledger technology could fit into the modern technologies bringing forth a positive and advancing change.

METHADOLOGY:

To implement the ideal All in One Digital Identity or say “Versatile Digital Identity” which is the combination of all the identities that represent a person, we must first understand how the government would do the deed.

1. How government could deliver Digital Identity:

ID systems gather and verify information to determine a person's identify and offer credential-based identification as confirmation of that identity, which is often a physical ID card, passport, or driver's license. Identity holders can use this to demonstrate their identity, for instance, to employers, financial institutions, or governmental organizations. Digital IDs are therefore the electronic equivalent of traditional identification. The credentials required to prove that a person is who they say they are online are provided by a digital ID. Significant advantages can result from a digital ID's capacity to streamline interactions between people, governments, and enterprises. **governments can deliver on the promise of digital ID**

1.1 Set up an effective operating model

The whole digital ID process, including user registration, authentication, and service provider integration, should be properly handled. Making the decision to "make or buy" early on is essential. The former sets up the system to be operated using a centralized paradigm, whilst the later results in a federated structure. In the centralized approach, the government is in charge of gathering data, creating digital credentials, and verifying user identities. To implement and run this, the required organizational and technical skills are needed. Since the system's introduction in 2002, Estonia, which has effectively established a centralized approach, has been the only provider, and it has successfully reached coverage of 99 percent of the population. In federated models, users are authenticated by a number of authorized identity providers who gather, manage, and store their characteristics and credentials. This strategy is especially advantageous if there is a large provider network with strong identity verification capabilities. This strategy has been used successfully in a number of countries, including Denmark, Finland, Norway, and Sweden, which all operate effective digital ID programs in partnership with banks. The choice of operating model may be influenced by the reliability and efficiency of the current digital ID infrastructure as well as the probable attitudes of the public toward private sector participation. Most significantly, governments have to think about selecting a model that is likely to promote quick registration and is based on a robust enough infrastructure to support increasing user numbers and authentications. A strong political commitment is necessary for success in both scenarios.

1.2 Ensure system interoperability

The environment in which a digital identity may be employed determines how beneficial it will be. An essential component is interoperability, or the ID system's ability to exchange data with other systems, databases, devices, and applications. Governments should prioritize ensuring interoperability across domestic business and public service providers as well as ID systems in foreign jurisdictions. Without interoperability, there is a danger that digital ID systems would lose steam and splinter as service providers create authentication methods tailored to their own requirements. To encourage seamless integration with service providers' systems and processes, interoperability at the service providing level is required. By using this method, individuals may, for instance, establish a company with a local government and purchase a customized ticket for public transportation. Some legal systems beyond their borders mandate interoperability. The EU's eIDAS Regulation, which mandates that all entities providing public digital services inside an EU member state accept electronic identity from other EU member states, is the most noteworthy example. Applications in the context of activities like travel, tourism, and immigration are expanded by compliance with these sorts of criteria. In order to achieve a high level of interoperability, two crucial actions must be taken. The first is adhering to standards in line with best practices used internationally. These can support interoperability in terms of data, which refers to the organization of information gathered and used by the system, and technology (such as biometrics, cards, and digital signatures). The second step involves putting technologies like technical interoperability layers, web services, and application programming interfaces into place to enable data transmission to and from other systems.

1.3 Establish a regulatory framework for broad usability

Creating a legislative framework that allows a wide range of use cases across the public and commercial sectors is difficult for lawmakers since it is necessary for widespread adoption by users and service providers. Governments should thus think about establishing the required regulations to facilitate use cases. For example, Estonia's regulatory foundations for cutting-edge digital ID systems render electronic authentication and signatures legally comparable to in-person identification and handwriting signatures. Avoiding undermining these fundamental equivalencies should be a top goal when developing legislation. Laws controlling the provision of particular services frequently have the consequence of reducing use. The necessity to deliver authentic papers that cannot be transferred online, such a visa or college graduation, or specific in-person requirements are common instances. Governments also need to handle any obstacles brought on by unexpected consequences of the ID system's requirements and supranational legislation. A requirement on banks under the EU's Fourth Anti-Money Laundering Directive to retain a record of how they vetted clients proved challenging to translate over to the scheme and hindered adoption of the solution for financial services in the UK's digital ID system. The EU's Fifth Anti-Money Laundering Directive addressed the problem. Governments must take action to create broad equivalency and alter laws that can forbid or restrict use cases in the public and private sectors.

1.4 Offer high-value use cases

Schemes for digital identification must genuinely benefit their users. This is not always easy because many people only interact with the government on average infrequently—just around five times a year in Germany, for instance. Governments should strive to include as many public-sector use cases as they can while concentrating on introducing enticing private-sector use cases as soon as feasible. Start with the processes that users find to be the most frequent or time-consuming, such as purchasing tickets for transportation and going through immigration at airports and railway stations. Additional features like digital vaults for private digital documents or electronic signatures may be needed for use cases that are more complicated. Additionally, governments have to think about providing incentives to service providers in the private sector. Entities that provide financial services are particularly appealing since many individuals utilize them. Banks offer many of the most effective programs, notably in Scandinavia. The private sector is where the Swedish BankID is used in about 91 percent of cases. There are several options, including age verification, digital licensing, and digital contract signing for commercial agreements.

2. Self-sovereign identity

An individual should own and govern their identity without the involvement of administrative authorities, according to the self-sovereign identity (SSI) movement, which is a phrase used to denote this idea. People may connect online with the same openness and capacity for trust that they do outside because to SSI. Everyone has diverse associations or distinctive sets of identifying information, including corporations and the Internet of Things. This data may include details such as birthdate, citizenship, academic credentials, or business licenses. These are reflected in the real world by cards and certificates that the identity holder keeps in their wallet or another secure location, such as a safety deposit box, and presents when asked to confirm their identity or something related to it. With its secure identity management platform, SSI extends the same liberties and individual freedoms to the internet. SSI denotes that the person (or entity) administers the components of their identity and restricts access to those credentials digitally. With SSI, the individual, not an administrative third party providing or monitoring access to these credentials, has authority over personal data. You can use your digital wallet and the credentials you were given to confirm your own identity with the SSI identification system. Every time you want to access new products and services, you no longer have to surrender control of your personal information to hundreds of databases, running the danger of having your identity stolen by hackers. Because each person now has authority over their own identity and is their own sovereign nation, this identity is known as "self-sovereign" identity. People are in charge of the connections and information in their lives. The digital life of an individual is now independent of any company; their identify cannot be removed.

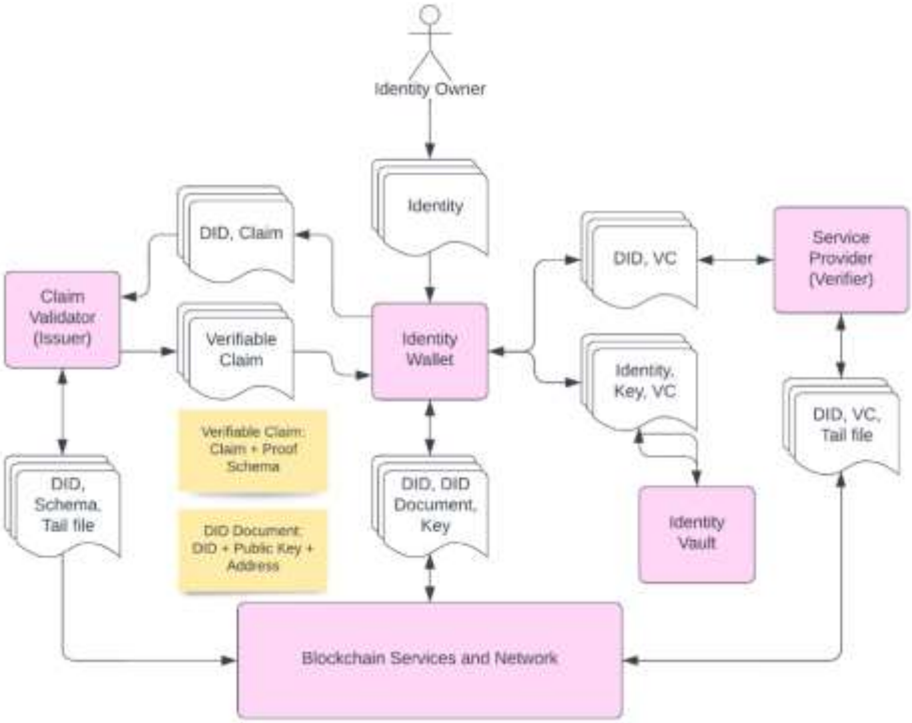

Fig. Self-Sovereign Identity Architecture

2.1 The idea of All-in-one identity

Similar to the self-sovereign identities, the idea of having all the possible identities of a person (such as Government issues id, license, passport, religion or caste, etc.) in one system to manage one single universal identity which represents the very existence of a person's being is the main idea of this paper. This would also include the records of one's deeds in the real life such as major accomplishments, certifications, or even collectibles such as NFTs that are linked to the Versatile digital identity. There is no hassle of maintaining all these records anymore. The system would be entirely coded on smart contracts on the public blockchain or government specified hybrid blockchain. This would make it so that credential issuing is fast and simple and could then be verified at any time and in any place regardless of whether or not the issuer still exists and is online. Credentials are made tamper-proof through cryptography. Digital identities are kept secret and in the user's control via selective identity disclosure technology. The user retains control of the interaction with the ID verifier and determines what information to divulge. Digital identities are kept secret and in the user's control via selective identity disclosure technology. The user retains control of the interaction with the ID verifier and determines what information to disclose. The connection between the ID issuer, the ID owner (the user), and the ID verifier takes place through a digital, secure peer-to-peer channel. Even the company that provides the SSI system is unaware of the information being exchanged. As the versatile digital identity employs a decentralized approach, it is considerably more difficult for threat actors to get into personal identifying information because it is not kept on a single server. Most of the time, you won't need to remember more than one password for several websites; all you need to remember is the one for your Versatile digital identity's digital wallet. Insecure, weak, and often used passwords can result from password fatigue, which is mitigated by doing this.

The issuer of the credential (a reputable entity), the ID verifier, and the owner of the digital ID (the user) form a triangle of trust in the versatile digital identity (typically a third party). The digital ID holder controls how and with whom their information is shared. To protect the privacy of the digital ID while enabling the ID holder to demonstrate that they comply with the standards, two major authentication techniques are utilized. This happens without revealing all of the personal data. The first technique is selective disclosure, which enables the user to produce proofs based on a small number of their credential's properties. They can demonstrate their age, for instance, by providing their birthday from a government-issued ID without also providing the rest of the information from the ID, which may include a personal address and other information. The zero-knowledge proof is the second authentication technique (ZKP). Through this approach, you may demonstrate with cryptography that the ID holder satisfies a criterion without actually disclosing the supporting data. When a link is created between the party issuing an ID and the ID's owner, the versatile digital identity would employ asymmetric encryption techniques that produce a public and private key. While the private (secret) key is used to validate the information, the public key is exchanged between the two parties. The digital wallet safely stores each of these connections.

CONCLUSION:

An evaluation of the applicability of an on-chain marketplace for digital products was conducted, first the current blockchain literature was reviewed and then a proof-of-concept artefact was designed. It was concluded that such approach is indeed feasible. The self-sovereign Identity was proposed where a user could have the permissions to make changes to their access modifiers on the information on his identity. The verify functions of the Smart Contract enables the authorities to verify the authenticity of the identity without actually revealing the information (readable by no one and verifiable by everyone).

This is a fully trustless process. The all-in-one identity was proposed to integrate multiple other identities into one to act as one whole Versatile Digital Identity. A portal could be made where the user could manage his identity. The Versatile Digital Identity brings forth many major possibilities. It could be used as the only proof necessary to create any online account on an application which could help prevent having multiple fake accounts. It could also be used to install the deeds of a person be it any major life accomplishments or criminal record. This could never be changed but could only have things added that might shadow the previous records.

References

[1]. P. Gellman, "Blockchain: The New Art House," in ITNOW, vol. 63, no. 3, pp. 18-19, Aug. 2021, doi: 10.1093/itnow/bwab070.

[2]. W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," in IEEE Access, vol. 7, pp. 134422-134433, 2019, doi: 10.1109/ACCESS.2019.2941905.

[3]. M. H. Mughal, Z. A. Shaikh, K. Ali, S. Ali and S. Hassan, "IPFS and Blockchain Based Reliability and Availability Improvement for Integrated Rivers' Streamflow Data," in IEEE Access, vol. 10, pp. 61101-61123, 2022, doi: 10.1109/ACCESS.2022.3178728.

[4]. Dib, Omar and Toumi, Khalifa, Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions (December 20, 2020). Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 19-40, Vol. 4, No. 5 (2020), Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2020.05.002.

[5]. J. S. Bellagarda and A. M. Abu-Mahfouz, "An Updated Survey on the Convergence of Distributed Ledger Technology and Artificial Intelligence: Current State, Major Challenges and Future Direction," in IEEE Access, vol. 10, pp. 50774-50793, 2022, doi: 10.1109/ACCESS.2022.3173297.

[6]. Z. Yang, H. Lei and W. Qian, "A Hybrid Formal Verification System in Coq for Ensuring the Reliability and Security of Ethereum-Based Service Smart Contracts," in IEEE Access, vol. 8, pp. 21411-21436, 2020, doi: 10.1109/ACCESS.2020.2969437.

[7]. M. Stefanović, Đ. Pržulj, S. Ristić, D. Stefanović and D. Nikolić, "Smart Contract Application for Managing Land Administration System Transactions," in IEEE Access, vol. 10, pp. 39154-39176, 2022, doi: 10.1109/ACCESS.2022.3164444.

[8]. S. Wang, R. Pei and Y. Zhang, "EIDM: A Ethereum-Based Cloud User Identity Management Protocol," in IEEE Access, vol. 7, pp. 115281-115291, 2019, doi: 10.1109/ACCESS.2019.2933989.

[9]. S. A. Gollapalli, G. Krishnamoorthy, N. S. Jagtap and R. Shaikh, "Land Registration System Using Block-chain," 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), 2020, pp. 242-247, doi: 10.1109/ICSIDEMPC49020.2020.9299606.

[10]. R. Kumar and R. Tripathi, "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain," 2019 Fifth International Conference on Image Information Processing (ICIIP), 2019, pp. 246-251, doi: 10.1109/ICIIP47207.2019.8985677.

[11]. B. Guidi, A. Michienzi and L. Ricci, "Data Persistence in Decentralized Social Applications: The IPFS approach," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021, pp. 1-4, doi: 10.1109/CCNC49032.2021.9369473.

[12]. S. Jianjun, L. Ming and M. Jingang, "Research and application of data sharing platform integrating Ethereum and IPFs Technology," 2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), 2020, pp. 279-282, doi: 10.1109/DCABES50732.2020.00079.